APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/829,499	04/22/2004	Cornell J. Kinderknecht	40003892-0056-002	6946

26263   7590   09/19/2008
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER
VU, TUAN A

ART UNIT	PAPER NUMBER
2193	

MAIL DATE	DELIVERY MODE
09/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _22 July 2008_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
     closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-33_ is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-33_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All b)☐ Some * c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
          application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to the Applicant's response filed 7/22/08.

        As indicated in Applicant's response, claims 1, 10, 22 have been amended. Claims 1-33

are pending in the office action.

Claim Rejections - 35 USC § 101

2.   35 U.S.C. 101 reads as follows:

   Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and
   useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3.   Claims 1-9 are rejected under 35 U.S.C. 101 because the claimed invention is directed to

non-statutory subject matter.

        The Federal Circuit has recently applied the practical application test in determining whether the claimed
subject matter is statutory under 35 U.S.C. § 101. The practical application test requires that a " useful, concrete,
and tangible result" be accomplished. An "abstract idea" when practically applied is eligible for a patent. As a
consequence, an invention, which is eligible for patenting under 35 U.S.C. § 101, is in the "useful arts" when it is a
machine, manufacture, process or composition of matter, which produces a concrete, tangible, and useful result. The
test for practical application is thus to determine whether the claimed invention produces a "useful, concrete and
tangible result".

        The current focus of the Patent Office in regard to statutory inventions under 35 U.S.C. § 101 for method claims and
claims that recite a judicial exception (software) is that the claimed invention recite a practical application. Practical application
can be provided by a physical transformation or a useful, concrete and tangible result. The following link on the World Wide
Web is the United States Patent And Trademark Office (USPTO) reference in terms of guidelines on a proper analysis on 35
U.S.C. §101 rejection.

<http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf>

        Specifically, claim 1 recites a system comprising an *injector*, a *redirect code* and *library*

of functions. As disclosed, the injector is a lightweight piece of pushed-down code

(Specifications pg. 5, top), and as claimed, the fact that the injector *is operable to be stored* in a

readable medium only depicts a storage possibility that does not necessarily include a readable

medium *into* the system. In whole, the elements recited amount to software in a system devoid

of any hardware storage or tangible embodiment so to realize the functionality of the software

elements, and this software listing amounts to 'Functional Descriptive Material' type of

deficiency (see USC101 Guidelines pdf file, Annex IV, pg. 52-54). The claimed subject matter

cannot be categorized as <u>any of the categories of statutory subject</u> matter (emphasis added); nor

can the claim, in the absence of hardware support, be deemed capable of realizing the listed

software material into real-world application data. The claim is rejected for non-statutory subject

matter for all of the above reasons.

Claims 2-9 for not providing hardware support to remedy to the above deficiency, are

also rejected for not fulfilling the statutory practical Application requirement as identified in part

by the USC § 101 Guidelines, as set forth above.

Claim Rejections - 35 USC § 112

4.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making
> and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it
> pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode
> contemplated by the inventor of carrying out his invention.

5.   Claims 1-33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with

the enablement requirement. The claim(s) contains subject matter which was not described in

the specification in such a way as to enable one skilled in the art to which it pertains, or with

which it is most nearly connected, to make and/or use the invention.

Specifically, claims 1, 10, 22 recite 'redirect code' performed by an *injector* and 'bypass

security in place at a remote computing system' (cl. 1, 4; cl. 10, li. 4; cl. 22, li. 8). The

Specifications mentions about remote control and 'bypass' a firewall in terms of being able to

access the otherwise firewall-controlled resources (para 0013, pg. 4); hence the remote computer

whose security in-place is to be bypassed is a firewall machine. Regarding using a injector

whereby some functionality of this firewall can be bypassed, the redirect code is illustrated in

Figure 3-4, and according to which, only after user's authentication with the firewall is achieved

can a injector be *pushed down* so to enable the user (behind the firewall) to launch application

(Specs: Fig. 4, 7-8) using said injector code. Disclosed is that this injector when deployed at the

user's machine intercepts, catch breakpoint, and/or redirect calls made within the user's

application or system low layers (Specs: Fig. 3-4), in terms of catching threads or socket calls, or

function calls then pointing to different spots of memory of the client application, or to dispatch

various control to other locations of that memory space (Fig. 4, 7-8). One of ordinary skill in the

art cannot see how security of the firewall (security in place) has been <u>bypassed</u> because a push-

down code enables a authenticated user to have low level calls redirected to other places of the

user application memory space. Eligibility of users behind a firewall for receiving a pushed

down code does not constitute a security bypass by any stretch. Actual bypassing of firewall

security is not depicted based on the push-down of the injector or interception of low level

system invocations as set forth above; that is, security is still maintained with the established

firewall in that only authenticated users are allowed to have the injector piece pushed to their

environment (Specs: Fig. 3) lest the whole purport of a firewall would be otherwise defeated.

The inventor is not deemed in possession of the means implementing how, using the injector

redirecting functionality, a given user has been able to clearly obviate security control performed

by the firewall (placed between the outside and the intranet users) in terms of the very claim

language ('bypass security in place at a remote computing system'): the security 'bypass' is

deemed not enabled by the Specifications. This limitation will be given no patentable merits

(emphasis added); and it would be treated in a broadest possible way as though the downloaded

injector performs interception and decryption tasks allowing secure assets inside the firewall to

be more easily accessed to a compliant intranet users.

Claims 10, 22 recite the 'bypass' limitation, and along with claims 2-9, 11-21, 23-33 are

rejected for not being provided with proper description from the Disclosure.

Claim Rejections - 35 USC § 102

6.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on
> sale in this country, more than one year prior to the date of application for patent in the United States.

7.   Claims 1-6, 10-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Calder et

al, USPubN: 2002/0092003(hereinafter Calder).

As per claim 1, Calder discloses a system for controlling an application process

comprising:

an injector operable stored on a computer readable medium (e.g. step 810, Fig. 8; para

0088, pg. 5 – Note: initializing package – step 540 Fig. 5 – reads on package having injector

code stored in client application); redirect code (step 540 Fig. 5; Fig. 9) operable to be placed in

a memory of the application process; and

a library of redirect functions operable to be referenced by the redirect code (e.g. step 920

- Fig. 9; para 0096, pg. 5; step 620, interception module 810 -Fig. 8; para 0103, pg. 6) during the

application process by the injector and

bypass security in place at a remote computing system (e.g. *approved network*

connection… participating client – para 0088, pg. 5 -Note: 'bypass' given weight only as

scenario wherein an eligible user in a network receives accessible data – see USC 112, 1st

paragraph; *transmitted ... to the client computer 140* – para 0092, pg. 5),

the redirect code operable to intercept a set of target function calls made by the

application process (intercept 940 - Fig. 9; para 103, pg. 6) and execute the redirect functions for

the intercepted target function calls (step 990 - Fig. 9).

As per claims 2-4, Calder discloses wherein the injector is pushed (interception module -

para 0096, pg. 5) to a device executing the application process; wherein the set of target function

calls comprises socket function calls (e.g. Fig. 27); wherein the library of redirect functions

comprises a dynamic link library (e.g. step 540-Fig.5; Fig. 9).

As per claim 5, Calder discloses: a secure environment having a plurality of resources

(e.g. *resource request 1335* - Fig. 13); a firewall securing all access to the plurality of resources

in the secure environment (e.g. Fig. 22-24, 26; para 0076 - pg. 4; Fig. 39-40); and an access

policy pushed to a device executing the application process, the access policy identifying the

resources authorized for access by the device (*access* - para 0074, pg. 3-4; Fig. 39-40 - Note: Lan

and internal network based on access checking and encryption of data reads on policy to deny

unauthorized intrusion).

As per claim 6, Calder discloses wherein the application process comprises an

application operable to communicate with the secure environment resources using an Internet

transport protocol, the redirect code, and the redirect functions (e.g. Fig. 1-4; Fig. 9; para 103,

pg. 6).

As per claim 10, Calder discloses a method for controlling an application process

comprising:

pushing an injector to a device executing the application process (Fig. 8);

injecting a redirect code into the application process (step 540 Fig. 5) and bypass security

in place at a remote computing system (e.g. *approved network connection… participating client*

– para 0088, pg. 5 -Note: 'bypass' given weight only as scenario wherein an eligible user in a

network receives accessible data – see USC 112, 1st paragraph; *transmitted … to the client*

computer 140 – para 0092, pg. 5),;

executing the redirect code in the application process to reference a redirect library (step

920 - Fig. 9; para 0096, pg. 5) of redirect functions;

resuming the execution of the application process (e.g. return - Fig. 36 - Note:

interception with handling via DLL entails a return back to the application after the handler code

has completed); and

intercepting at least one target function calls made by the application process and

executing at least one redirect function (step 990 - Fig. 9) in place of the at least one target

function calls.

As per claim 11, Calder discloses: starting the application process; interrupting the

execution of the application process; and injecting the redirect code into a memory space of the

application process (Fig. 10-11).

As per claim 12, Calder discloses wherein injecting a redirect code further comprises:

starting the application process using a debug option; catching an exception thrown by the

application process; locating memory space in the application process; injecting the redirect code

into the memory space of the application process; and set an instruction pointer to the redirect

code (e.g. step 1030 - Fig. 10; Fig. 15, 33, 41).

As per claim 13, Calder discloses wherein injecting a redirect code further comprises: starting the application process using a suspend option; creating memory space in the application process; injecting the redirect code into the memory space of the application process; and set an instruction pointer to the redirect code (e.g. Fig. 7, 10-11).

As per claim 14, Calder discloses wherein injecting a redirect code further comprises: starting the application process using a suspend option; creating memory space in the application process; injecting the redirect code into the memory space of the application process; (Fig. 7, 10-11); and use a create remote thread function to execute the redirect code (e.g. Fig. 13; Fig. 15).

As per claim 15, Calder discloses wherein executing the redirect code comprises: loading the redirect library of redirect functions; determining a location of an import table replacement (Fig. 7,10 - Note: import table, export table reads on table of routines to insert to memory for replacement) function in the redirect library; and executing the import table replacement function.

As per claim 16, Calder discloses table including a dynamic link library (Fig. 10-11).

As per claim 17, Calder discloses wherein executing the import table replacement function comprises: searching an import table of the application process for the set of target function calls; and modifying the target function calls to reference redirect functions in the redirect library (Fig. 10-11).

As per claim 18 Calder discloses wherein executing the import table replacement function comprises: searching dynamic link libraries of the application process for the set of target function calls; and modifying the target function calls to reference redirect functions in the redirect library (e.g. para 0102, pg. 6).

    As per claims 19-21, Calder discloses receiving user information; authenticating the user information; pushing an access policy specifying resources accessible by a user associated with the user information to a device used by the user; executing redirect functions to enable a secured access to a plurality of resources via a firewall (refer to claim 5)

    As per claim 20, refer to claim 3

    As per claim 22, Calder discloses method comprising:

    receiving user information; authenticating the user information (Fig. 18-19; re claim 5);

    pushing an injector to a device executing an application process (Fig. 8); and

    intercepting at least one target function call made by the application process to at least one of a plurality of secure resources and executing at least one redirect function in place of the at least one target function call (step 540 Fig. 5; step 920 - Fig. 9; para 0096, pg. 5) and

    bypass security in place at a remote computing system (e.g. *approved network connection... participating client* – para 0088, pg. 5 -Note: 'bypass' given weight only as scenario wherein an eligible user in a network receives accessible data – see USC 112, 1st paragraph; *transmitted ... to the client computer 140* – para 0092, pg. 5),.

    As per claim 23, Calder discloses: injecting a redirect code into the application process; executing the redirect code in the application process to reference a redirect library of redirect functions; and resuming the execution of the application process (see claim 10).

    As per claims 24-27, refer to claim 11-14, respectively.

    As per claims 28-31, refer to claim 15-18, respectively

    As per claims 32-33, refer to claim 20-21, respectively

                            Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102
of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject
matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art
to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9.   Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Calder et al,

USPubN: 2002/0092003, and further in view of Thomas et al., USPN: 6,148,336 (hereinafter

Thomas).

        As per claim 7, Calder does not explicitly disclose wherein the application process

comprises an email application. But GUI-based applications for which resources request are

being fulfilled to support user's applications is disclosed (see Fig. 33-34; Fig. 47) in Calder's

network of Lan users. Users applications having interception of messages with insertion of

special code to redirect to a proper validating or readdressing of message request is disclosed in

Thomas's Web-based paradigm (e.g. Fig. 6; *library ... containing a plug-in* - col. 9, lines 6-40)

wherein socket communications are inserted with a plug-in supported via a DLL container for

redirection with proper binding and re-wrapping (see Fig. 9-10). Based on Thomas' approach to

introduce a novel way for addressing IP address filtering drawback wherein Email is one such

application involving such filtering concern (see col. 2), it would have been obvious for one skill

in the art to implement the application examination by Calder (see Fig. 33-34; *decrypt* - Fig. 39)

so that the interception of LAN network messages via IP/TCP protocol via some dynamic

application extension (such as plug-in as by Thomas -- see SUMMARY of Invention - col. 4-5)

would be able examine the likes of Email message content and resolve potential incompatibility

issues by this extension service such as examining, blocking, modifying, decrypting and re-

encrypting prior to providing a wrap-up binding process (see Thomas, col. 5) which also

endeavored as set forth above by Calder.

　　　　As per claims 8-9, Calder does not disclose wherein the application process comprises a

web browser application wherein the application process comprises a file transfer application.

But applications with Winsock (see Thomas (see Fig. 1-6) or Windows system having provision

of Dlls (see Calder para 0081-0082) was known environments in which standard file transfer

and browser applications would have founded to provide communications between users and

services. The limitation that applications be Email, or FTP or browser messages in light of the

interception and redirection as taught by both Calder and Thomas would have been obvious for

the same rationale as set forth above, because application like those require message transfer

using a proper protocol, and the interception as purported by Calder or Thomas would support

examination of such message internals to provide a modified and adjusted redirection as

mentioned above in the respective endeavor by Calder and Thomas.

                                             Response to Arguments

10.　　　Applicant's arguments filed 7/22/08 have been fully considered but they are MOOT

and/or not persuasive. Following are the Examiner's observation in regard thereto.

(A)　　　Applicants have submitted that Calder does not teach 'placed in a memory of the

application process' and 'bypass security ... computing system' (Appl. Rmrks pg. 9, 2nd para).

The added limitations (e.g. bypassing security, storage medium) have necessitated readjustment

in the present Office Action; hence the argument is moot because it would be deemed not

responsive to the previous Office Action.

(B)   Applicants have submitted that Thomas does not cure to the deficiency of Calder (Appl.

Rmrks pg. 9, bottom).   The rationale of rejection using Thomas is not aimed at addressing

'bypass security' and Applicant fail to point to exactly where in the 103 obviousness rationale

any factual deficiency thereof in terms of (i) counter-teaching; (ii) undesirable result or (iii)

inapposite juxtaposition of non-analogous technologies, (iv) how all of which amount to failure

to achieve the claim as a whole. The argument is mere allegation against one reference only; and

in response to applicant's arguments against the references individually, one cannot show

nonobviousness by attacking references individually where the rejections are based on

combinations of references. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re

Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

        In all, the claims (including the non-statutory rejection) stand rejected as set forth in the

Office Action.

Conclusion

11.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tuan A Vu whose telephone number is (571) 272-3735. The

examiner can normally be reached on 8AM-4:30PM/Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Lewis Bullock can be reached on (571)272-3759.

The fax phone number for the organization where this application or proceeding is

assigned is (571) 273-3735 (non-official correspondence - please consult Examiner before

using) or 571-273-8300 (for official correspondence) or redirected to customer service at 571-

272-3609.

Any inquiry of a general nature or relating to the status of this application should be

directed to the TC 2100 Group receptionist: 571-272-2100.

Information regarding the status of an application may be obtained from the Patent Application
Information Retrieval (PAIR) system. Status information for published applications may be
obtained from either Private PAIR or Public PAIR. Status information for unpublished
applications is available through Private PAIR only. For more information about the PAIR
system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR
system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Tuan A Vu/

Primary Examiner, Art Unit 2193

September 16, 2008